SAFER • HEALTHIER • PEOPLE™

NATIONAL HEALTHCARE SAFETY NETWORK
FACILITY/GROUP ADMINISTRATOR
RULES OF BEHAVIOR

Version 1.0

08/08/05

VERSION HISTORY

Version #	Implemented By	Revision Date	Reason
1.0	James Tolson	08/08/05	

TABLE OF CONTENTS

1 INTRODUCTION

NHSN, a surveillance system of the Centers for Disease Control and Prevention (CDC), allows participating healthcare facilities to enter data associated with healthcare safety, such as surgical site infections, antimicrobial use and resistance, bloodstream infections, dialysis incidents, and healthcare worker vaccinations. NHSN provides analysis tools that generate reports using the aggregated data (reports about infection rates, national and local comparisons, etc). NHSN also provides links to best practices, guidelines, and lessons learned.

NHSN processes and stores a variety of sensitive data that are provided by healthcare facilities. This information requires protection from unauthorized access, disclosure, or modification based on confidentiality, integrity, and availability requirements. These "Rules of Behavior" apply to all users of the NHSN web-based computer system.

1.1 PURPOSE

Rules of Behavior establish standards that recognize knowledgeable users are the foundation of a successful security plan. Non-compliance with these rules will be enforced through sanctions equal to the level of infraction. Sanctions can include a written or verbal warning and possible removal of system access. NHSN will enforce the use of penalties against any user who willfully violates any NHSN or federal system security (and related) policy as appropriate. Users are also responsible for reporting security incidents, or any incidents of suspected fraud, waste, or misuse of NHSN systems to the CDC NHSN administrator.

The objective of the NHSN Rules of Behavior document is to summarize laws and guidelines from HHS and other Federal documents, most specifically OMB Circular A-130, Subsection (m) of the Privacy Act of 1974 (U.S.C. 552a) and Section 308(d) of the Public Health Service Act (U.S.C. 242m). It defines the rules of behavior in terms of policy and responsibility for the intended audience of CDC NHSN team members and NHSN facility/group member users.

1.2 DEFINITIONS

1.2.1 What are Rules of Behavior?

Rules of behavior are part of a comprehensive program to provide complete information security. These guidelines were established to hold users accountable for their actions and responsible for information security. Rules of behavior establish behavioral standards in recognition of the fact that knowledgeable users are the foundation of a successful security program.

1.2.2 Who is Covered by these Rules?

These rules extend to CDC NHSN team members and their authorized contractors and agents (e.g., guest researchers, students) and NHSN facility/group member users.

The rules of behavior are not to be used in place of existing policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing

NHSN. The rules are consistent with the policy and procedures described in this document, and include but are not limited to, the following directives:

- Privacy Act
- Freedom of Information Act
- Section 508 of the Workforce Investment Act of 1998
- Computer Security Act Public Law 100-235
- E-Government Act Public Law 107-347
- Paperwork Reduction Act of 1995
- Clinger-Cohen Act of 1996
- CDC's Public Health Information Network (PHIN)
- CDC's Secure Data Network (SDN)
- National Institute of Standards and Technology (NIST) publications
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- HHS AISSP Handbook
- Member-specific data security, privacy and confidentiality regulations, policies
- State statutes.

1.2.3 What are Penalties for Non-compliance?

Non-compliance with these rules will be enforced through sanctions appropriate with the level of infraction. Users who do not comply with the prescribed Rules of Behavior are subject to penalties that can be imposed under existing policy and regulation, including suspension of system privileges.

1.3 REFERENCES

[1] Office of Management and Budget. Circular No. A-130, Revised, (Transmittal Memorandum No. 4): Management of Federal Information Resources. August 31, 2004. http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html.

[2] Center for Information Technology, National Institutes of Health, NIH Information Technology General Rules of Behavior. August 31, 2004. http://wwwoirm.nih.gov/security/nihitrob.html#general

[3] The Privacy Act of 1974, 5 USC § 552a -- As Amended. August 31, 2004. http://www.usdoj.gov/foia/privstat.htm

[4] The Freedom of Information Act 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048. August 31, 2004. http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm

[5] Section 508 of the Workforce Investment Act of 1998. August 31, 2004. http://www.section508.gov/index.cfm?FuseAction=Content&ID=3

[6] Computer Security Act Public Law 100-235. August 31, 2004. http://cio.doe.gov/Documents/CSA.HTM

[7] E-Government Act Public Law 107-347. August 31, 2004. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107

[8] Paperwork Reduction Act of 1995. August 31, 2004. http://www.archives.gov/federal_register/public_laws/paperwork_reduction_act/3501.html

[9] Clinger-Cohen Act of 1996. August 31, 2004. http://wwwoirm.nih.gov/policy/itmra.html

[10] PHIN Compatibility. August 31, 2004. http://www.cdc.gov/phin/

[11] SDN. August 31, 2004. http://www.cdc.gov/irmo/ea/sdn.htm

[12] NIST. August 31, 2004. http://nvl.nist.gov/

[13] HIPAA. September 8, 2004 http://hipaa.org

[14] HHS AISSP Handbook. September 8, 2004.

2 POLICY RULES

2.1 LEGAL, REGULATORY, AND POLICY REQUIREMENTS

Information handled by the system includes sensitive information about a member facility and its patients and/or healthcare personnel. The loss, misuse, or unauthorized access to or modification of information in the system could result in a loss of confidentiality or privacy. If integrity of NHSN data were adversely affected, it would negatively impact decision-making and scientific data analysis.

2.2 STATEMENT OF SYSTEM POLICY

Each user is responsible for helping to prevent unauthorized use of, and access to, system resources. This duty includes complying with all stated policy requirements, taking due care and reasonable precautions when handling system data or using system resources, and in the management and protection of system authentication controls (passwords, digital certificates, etc.). When in doubt, users are strongly encouraged to contact the SDN help desk or NHSN help desk (see Contact Information table, Section 4, Page 11).

CDC SDN and NHSN administrators may periodically monitor both the system and user activities for purposes including, but not limited to, troubleshooting, performance assessment, usage patterns, indications of attack or misuse and the investigation of a complaint or suspected security incident. Users are provided access to the NHSN through the SDN for the purpose of facilitating CDC's public health mission. Because CDC is responsible for maintaining security for all systems accessible through the SDN, it has the authority under federal and state laws to monitor all users' communications on the SDN, even with remote equipment. This statutory authority is based on ensuring the appropriateness of such communications and for that purpose random computer checks may be done.

3 USER RESPONSIBILITIES

3.1 ETHICAL CONDUCT

NHSN stores a variety of sensitive data. This sensitive information requires protection from unauthorized access, disclosure, or modification based on confidentiality, integrity, and availability requirements. System users should exercise due care to preserve data integrity and confidentiality and take reasonable precautions to ensure the protection of data from unauthorized access or use.

Specifically, any personally identifiable information entered into this system must not be used for anything other than the intended purpose. System administrators are to ethically conduct all monitoring activities and avoid any unnecessary or unauthorized breach of user privacy.

3.2 AUTHENTICATION MANAGEMENT

Users will access NHSN through the CDC Secure Data Network (SDN). Users will ensure the security of their SDN Digital Certificate and pass phrase. Users who believe their SDN Digital Certificate or SDN pass phrase have been compromised in any way will immediately inform the SDN Help Desk. Users will supply an SDN pass phrase that meets the SDN pass phrase requirements. Sharing of a SDN Digital Certificate and/or SDN pass phrase is strictly prohibited. Once logged into the Secure Data Network each NHSN user will have a unique User Name and password for the NHSN system. Each user is responsible for protecting their password. Passwords should not be shared as users are responsible for all actions performed with their account. Passwords must be at least seven characters in length and must contain at least one capital letter, one lower case letter, and one number. System and State administrators will never ask for your password and cannot retrieve your password for you. Each user is required to report to administrators immediately upon discovery of their account credentials being compromised or suspect they have been compromised.

3.3 INFORMATION MANAGEMENT AND DOCUMENT HANDLING

Hard copy system documents (i.e. reports, print-outs, etc.) should be handled in a way that conforms to federal or state data security, privacy and confidentiality regulations, policies and statutes.

3.4 GENERAL SYSTEM ACCESS AND USAGE

When a facility or group is enrolled into NHSN, CDC will assign to it an NHSN facility ID number or NHSN group ID number, and instruct the facility/group administrator to obtain a digital certificate for accessing the NHSN through the CDC's Secure Data Network.

Facility/group administrators are initially given access rights upon activation of their facility/group in the NHSN (final step of the enrollment process). Administrators have all access rights and can update facility/group information and add, modify, and delete users within their facility/group, as well as assign those users specific roles and access rights.

Users are required to notify the Facility/group administrator of changes in job status that might affect the appropriateness of continued access.

Users are assigned roles and accompanying access rights to various parts of the application by their NHSN facility administrator. Roles include that of Analyst, Data Reporter or both. The role of Administrator can also be granted to a user. The CDC NHSN administrator has access rights to all data in all facilities.

- Users will access the system through CDC's SDN.
- A SDN digital certificate must be obtained before a user can access the system. The user must also be approved to access the NHSN program within the SDN.
- The user is responsible for notifying NHSN facility/group administrator or CDC NHSN administrator of any changes in job status (promotion, demotion, transfer, termination, etc.) that might affect the appropriateness of continued access.

3.5 AWARENESS AND GENERAL INCIDENT REPORTING

Facility administrators should be vigilant for and have responsibility for reporting suspicious events, system misuse, suspected compromise or loss. These should be reported to the CDC NHSN administrator at 1-800-893-0485 or via email at nhsn@cdc.gov.

3.6 TRAINING

NHSN facility administrators should train themselves and their users using this document and other available materials regarding the need for and how to maintain system security.

3.7 PROHIBITIONS

System users are prohibited from the disclosure of information about the system, its architecture, function, or security controls and may not attempt to bypass system security controls. Also, users are prohibited from any activity that conflicts with local data security and confidentiality.

- Do not attempt to access any data or programs on the NHSN system for which you do not have authorization.
- Do not engage in, encourage, conceal any "hacking" or "cracking," denial of service, unauthorized tampering, or unauthorized attempted use of (or deliberate disruption of) any computer system within the NHSN system.
- Do not purposely engage in any activity with the intent to:
  - Degrade the performance of the system
  - Deprive an authorized user access to a resource

- Obtain or attempt to obtain extra resources beyond those allocated
- Circumvent security measures in order to gain access to any automated system for which proper authorization has not been granted.

3.8 ADDITIONAL RULES FOR ADMINISTRATORS

Facility and group administrators have added responsibilities to ensure the secure operation of NHSN.

3.8.1.1 Specific Responsibilities

- Ensure that adequate physical and administrative safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorize personnel, on a need to know basis.

- Verify that users have received appropriate security training before allowing access to NHSN.

- Document and investigate known or suspected security incidents or violations and report them to the NCID ISSO, CISO, and systems owner.

4 USER ASSISTANCE AND ADDITIONAL RESOURCES

To obtain system-related assistance (help desk, vendor support, system management, etc.) users should contact one of the following:

Name	Telephone	Email
SDN Help Desk	800-532-9929 or 770-216-1276	cdcsdn@cdc.gov
NHSN Help Desk	800-893-0485	nhsn@cdc.gov

5 REVISIONS AND RENEWAL

When new versions of this document are released, the system business or technical steward will provide a revised copy to all users and request an acknowledgement of receipt. If users do not provide an acknowledgement or feedback within a reasonable time, they will be considered to have given tacit approval to the revised document. User comments, feedback, questions, or objections will be considered for integration into further revisions.

6 ACKNOWLEDGEMENT AND AGREEMENT

I have read and agree to comply with the terms and condition governing the appropriate and allowed use of NHSN as defined by this document, applicable agency policy, and Federal law. I understand that infractions of these rules will be considered violations of CDC standards of conduct and may result in disciplinary action including the possibility of supervisory notification, suspension of system privileges, and/or criminal and civil prosecution.

The act of acknowledgement and agreement signifies a clear understanding of the NHSN Rules of Behavior document and that the signer will conform to the rules provided therein.

I acknowledge receipt of, understand my responsibilities, and will comply with the rules of behavior for NHSN.

Signature **Date**

Printed Name